REMARKS

By this Amendment, claims 33-45 and 52-58 are cancelled, and claims 46, 48, 50 and 51 are amended. Claims 47-49 remain in the application. Thus, claims 46-51 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

A first Amendment After Final was filed in the present application on January 31, 2006. However, the Examiner prevented entry of the January 31, 2006 Amendment After Final in an Advisory Action dated February 17, 2006 because the arguments presented in the first Amendment After Final would require further searching and consideration.

The present Second Amendment After Final is entered in favor of the first Amendment After Final through the filing of a Request for Continued Examination. Accordingly, the Applicants respectfully request that the present application proceed on the basis of the present Second Amendment After Final.

Rejection of Claims

I. In item 9 on page 3 of the Office Action, claims 33-45 were rejected under 35 U.S.C. § 102(a) as being anticipated by Woolsey et al. (U.S. 6,029,000, hereinafter "Woolsey"). This rejection is believed to be moot in view of the cancellation of claims 33-45.

II. In item 12 on page 9 of the Office Action, claims 46, 52 and 57-58 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Woolsey view of Gong et al. (NPL "Going Beyond the Sandbox: An Overview of The New Security Architecture in The JAVA Development Kit 1.2, hereinafter "Gong"). This rejection is believed to be moot with respect to claims 52 and 57-58 in view of the cancellation of claims 52 and 57-58.

Without intending to acquiesce to this rejection, independent claim 46 has been amended to more clearly illustrate the marked differences between the present invention and the applied references.

Claim 46 recites a data processor for receiving and processing data to which information for tampering detection is added. The data processor of claim 46 includes the following features (A) to (C):

(A) The data processor of claim 46 comprises a receiver operable to receive data which includes an authentication information region for including the tampering detection region, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data not to be subjected to tampering detection. Further, claim 46 defines that the protected data region includes an unprotection list which lists, by type, the data included in the unprotected data region.

(B) The data processor of claim 46 comprises a protected data authentication unit operable to detect, for the data which is included in the protected data region and received by the receiver, whether the data included in the protected data region has been tampered with by using the tampering detection information included in the authentication information region.

(C) The data processor of claim 46 also comprises an unprotected data authentication unit operable to determine the data included in the unprotected data region as being valid when a data type of the data, which is included in the unprotected data region and received by the receiver, coincides with a data type in the unprotection list which has been confirmed as not having been tampered with by the protected data authentication unit.

Accordingly, the data processor of claim 46 provides that unprotected data (i.e., data not subject to encryption) is determined to be valid when the unprotected data has a data type which coincides with a data type that has been confirmed as not having been tampered with.

In particular, the data processor of claim 46 determines that the data included in the unprotected data region is valid when a data type of the data, which is included in the unprotected data region and received by the receiver, coincides with a data type in the unprotection list which has been confirmed as not having been tampered with the by the protected data authentication unit. Therefore, the data processor as recited in claim 46 increases the reliability of data in the unprotected data region (i.e., data not subject to encryption) by determining whether the data included in the unprotected data region is valid based on whether a data type of the data included in the unprotected data region coincides with a data type in the unprotection list which has been confirmed as not having been tampered with.

As described above, the protected data authentication unit confirms whether the unprotection list has been tampered with. Therefore, according to the data processor recited in claim 46, if a data type of the data included in the unprotected data region does not coincide with the data type in the unprotection list that has been confirmed as not having been tampered with by the protected data authentication unit, the data is determined to be unreliable and is then discarded. Consequently, the reliability of data included in the unprotected data region and received by the receiver is increased. Furthermore, since the unprotection list is merely a list in which the data included in the unprotected data region is listed by type, encrypting the unprotection list does not take a lot of time.

Therefore, the present invention provides a novel, remarkable and advantageous effect in which the validity of data in the unprotected data region and received by the receiver is verified in a simple manner which does not prolong the amount of time for encrypting the unprotection list.

The Applicants respectfully submit that the applied references do not disclose or suggest the above-described features (A) to (C) recited in claim 46 and the aforementioned effects achieved therefrom.

In the Advisory Action, the Examiner asserted that Woolsey and Gong disclose the receiver and unprotected data authentication unit. However, the Applicants respectfully submit that Woolsey and Gong do not disclose the receiver and unprotected data authentication unit of claim 46 for the following reasons.

Woolsey discloses a mobile communication system in which an applet is encrypted. In the mobile communication system of Woolsey, a processor downloads, via a network, an applet which has been signed and encrypted, and then verifies whether or not a signature of the applet is valid based on a list of trusted sources. If the signature is determined to be valid, the processor decrypts the encrypted applet (see Column 20, line 50 to Column 21, line 17).

Gong discloses JDK1.1 and JDK1.2 security models. Gong discloses that when an applet is received, the JDK1.1 security model (or JDK1.2 security model) verifies a signature of the applet, and, if the signature is determined to be valid, permits the applet to access resources of a computer having received the applet.

Accordingly, Woolsey and Gong merely disclose a technique of authenticating a signature that is received at a receiving end. As acknowledged by the Examiner, Woolsey clearly does not disclose or suggest a receiver operable to receive a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data that is not to be subjected to tampering detection. In an attempt to teach this feature, the Examiner applied Gong, which discloses granular permissions in JAVA. However, the granular permissions in JAVA as disclosed in Gong provide no reasonable basis for interpreting that Gong receives a protected data region that includes an unprotection list which lists, by type, the data included in the unprotected data region. Instead, the granular permissions in JAVA as disclosed in Gong merely determine whether a signature of a received applet is valid based on whether keys indicate an authenticated source of the applet or whether a source of the applet is authentic (see, for example, the paragraph spanning pages 3-4 of Gong).

Despite the Examiner's assertion to the contrary, Gong clearly does not disclose or suggest that a receiver receives a protected data region that includes an unprotection list which lists, by type, the data included in an unprotected data region, as recited in claim 46.

Moreover, as described above, the techniques of Woolsey and Gong are merely for authenticating a received signature. The techniques of Woolsey and Gong do not, however, determine whether received data, which is included in an unprotected data region, is valid by determining whether a data type of the data included in the unprotected data region coincides with a data type in an unprotection list which as been confirmed as not having been tampered with, as recited in claim 46.

Accordingly, Woolsey and Gong clearly do not disclose or suggest an unprotected data region operable to determine the data included in the unprotected data region as being valid when a data type of the data, which is included in the unprotected data region and received by the receiver, coincides with a data type in the unprotection list which has been confirmed as not having been tampered with by the protected data authentication unit, as recited in claim 46.

Therefore, no obvious combination of Woolsey and Gong would result in the invention of claim 46 since Woolsey and Gong, either individually or in combination,

clearly fail to disclose or suggest the receiver and unprotected data authentication unit as recited in claim 46.

Thus, the Applicants respectfully submit that claim 46 is clearly patentable over Woolsey and Gong.

III. In item 10 on page 6 of the Office Action, claims 48-51 were rejected under 35 U.S.C. § 102(e) as being anticipated by Kolouch (U.S. 6,694,433). Without intending to acquiesce to this rejection, independent claims 48, 50 and 51 have each been amended in order to more clearly illustrate the marked differences between the present invention and the applied references.

In particular, claims 48, 50 and 51 have each been amended to include limitations similar to features (A) to (C) described above with respect to claim 46.

Claim 48 recites a data processor structured by a transmitting data processor and a receiver data processor, where the transmitting data processor is operable to transfer, to the receiving data processor, data to which information for tampering detection is added.

The data processor of claim 48 is recited as comprising the protected data authentication unit and the unprotected data authentication unit of claim 46.

Claim 50 recites a data processing method which performs operations similar to those of the data processor of claim 46. Claim 51 also recites a data processing method which performs operations similar to those of the data processor of claim 48.

Claims 48, 50 and 51 therefore each recite limitations substantially similar to features (A)-(C) described above with respect to claim 46.

As demonstrated above, Woolsey and Gong clearly do not disclose a receiver or receiving operation for receiving a protected data region that includes an unprotection list which lists, by type, the data included in an unprotected data region.

As also demonstrated above, Woolsey and Gong clearly do not disclose or suggest an unprotection data authentication unit or method operation for determining whether received data, which is included in an unprotected data region, is valid by determining whether a data type of the data included in the unprotected data region coincides with a data type in an unprotection list which as been confirmed as not having been tampered with.

In the Advisory Action, the Examiner asserted that Kolouch discloses the combination of unprotected list generation unit, the data generation unit and the unprotected data authentication unit, as recited in claim 48 and as similarly recited in the method of claim 51.

However, the Applicants respectfully submit that Kolouch clearly does not disclose the above combination. Kolouch discloses a XML encryption scheme in which a part of a XML file is encrypted and the remaining part of the XML file is not encrypted. Figure 5 of Kolouch shows that an encrypted object is embedded within another object (see Column 4, lines 53-62 and Column 5, lines 34-42).

This is markedly different from creating a list which lists, by type, unprotected data, as recited in claims 48 and 51. Similarly, the above disclosure of Kolouch is markedly different from receiving a protected data region that includes an unprotected list which lists, by type, the data that is included in the unprotected data region, as recited in claims 46 and 50. In fact, Kolouch does not disclose, suggest or even contemplate the principal purpose of the inventions of claims 46, 48, 50 and 51, which is to increase the reliability of data in an unprotected data region (i.e., data that is not subject to encryption).

Moreover, the Applicants respectfully submit that Kolouch clearly fails to disclose or suggest determining whether received data, which is included in an unprotected data region, is valid by determining whether a data type of the data included in the unprotected data region coincides with a data type in an unprotection list which as been confirmed as not having been tampered with, as recited in claims 46, 48, 50 and 51.

Therefore, similar to Woolsey and Gong, Kolouch clearly fails to disclose features (A) to (C) described above, as recited in claims 46, 48, 50 and 51. Consequently, no obvious combination of Woolsey, Gong and Kolouch would result in the inventions of claims 46, 48, 50 and 51 since Woolsey, Gong and Kolouch, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 46, 48, 50 and 51.

Although not applied in the Office Action, the Examiner cited Cofta (U.S. Patent Application Publication No. 2001/0016042), Shear (U.S. 6,157,721) and Atkinson (U.S. 5,892,904). However, similar to Woolsey, Gong and Kolouch, Cofta, Shear and

Atkinson also each fail to disclose or suggest features (A) to (C) as recited in claims 46, 48, 50 and 51.

Therefore, no obvious combination of Woolsey, Gong, Kolouch, Cofta, Shear and Atkinson would result in the inventions of claims 46, 48, 50 and 51 since Woolsey, Gong, Kolouch, Cofta, Shear, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 46, 48, 50 and 51.

Because of the clear distinctions discussed above, it is submitted that the teachings of Woolsey, Gong, Kolouch, Cofta, Shear clearly do not meet each and every limitation of claims 46, 48, 50 and 51.

Furthermore, it is submitted that the distinctions are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Woolsey, Gong, Kolouch, Cofta, Shear in such as manner as to result in, or otherwise render obvious, the present invention as recited in claims 46, 48, 50 and 51.

Therefore, it is submitted that the claims 46, 48, 50 and 51, as well as claims 47 and 49 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

A fee and a Petition for a two-month Extension of Time are filed herewith pursuant to 37 CFR § 1.136(a).

Respectfully submitted,

Takuya KOBAYASHI et al.

By: _____
Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
April 3, 2006